



SPYWOLF

Security Audit Report



Completed on
June 14, 2022

MADE IN USA 

 @SPYWOLFNETWORK

 @SPYWOLFNETWORK

 SPYWOLF.CO



OVERVIEW

This audit has been prepared for **Double Eagle** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03-04
Featured Wallets	05
Vulnerability Check	06
Threat Levels	07
Found Threats	08
Good Practices	09
Tokenomics	10
Team Information	11
Website Analysis	12
Social Media & Online Presence	13
About SPYWOLF	14
Disclaimer	15



Double Eagle



PROJECT DESCRIPTION

According to their whitepaper:

Double eagle protocol is a distributed financial service platform based on binance smart chain. The protocol design is based on compound and DAO architecture. The double eagle platform will include modules such as lending, governance and mining.

The protocol allows users to borrow and repay money at any time.

Release Date: July 14, 2021

Category: Lending



CONTRACT INFO

Token Name
Double eagle

Symbol
DOE

Contract Address
0x6Cb2a064435B4776374C0A3b252e294468993A2D

Network
Binance Smart Chain

Language
Solidity

Deployment Date
May 27, 2022

Verified?
Yes

Total Supply
30,000,000

Status
Launched

TAXES

Buy Tax
4%

Sell Tax
6%

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



CURRENT STATS

(AS OF July 14, 2022)



Liquidity

PancakeSwap:
2 907 USDT



Burn

None

Status:
Launched!

MaxTxAmount
No limit

No additional info

LP Address(es)

Pancakeswap:

0x0B35a604004867E774D0C919FfFC724c05971d0f

100% Unlocked



TOKEN TRANSFERS STATS

Transfer Count	2457
Uniq Senders	672
Uniq Receivers	1234
Total Amount	35115165 DOE
Median Transfer Amount	4.999 DOE
Average Transfer Amount	14291 DOE
First transfer date	2022-05-27
Last transfer date	2022-06-14
Days token transferred	18

SMART CONTRACT STATS

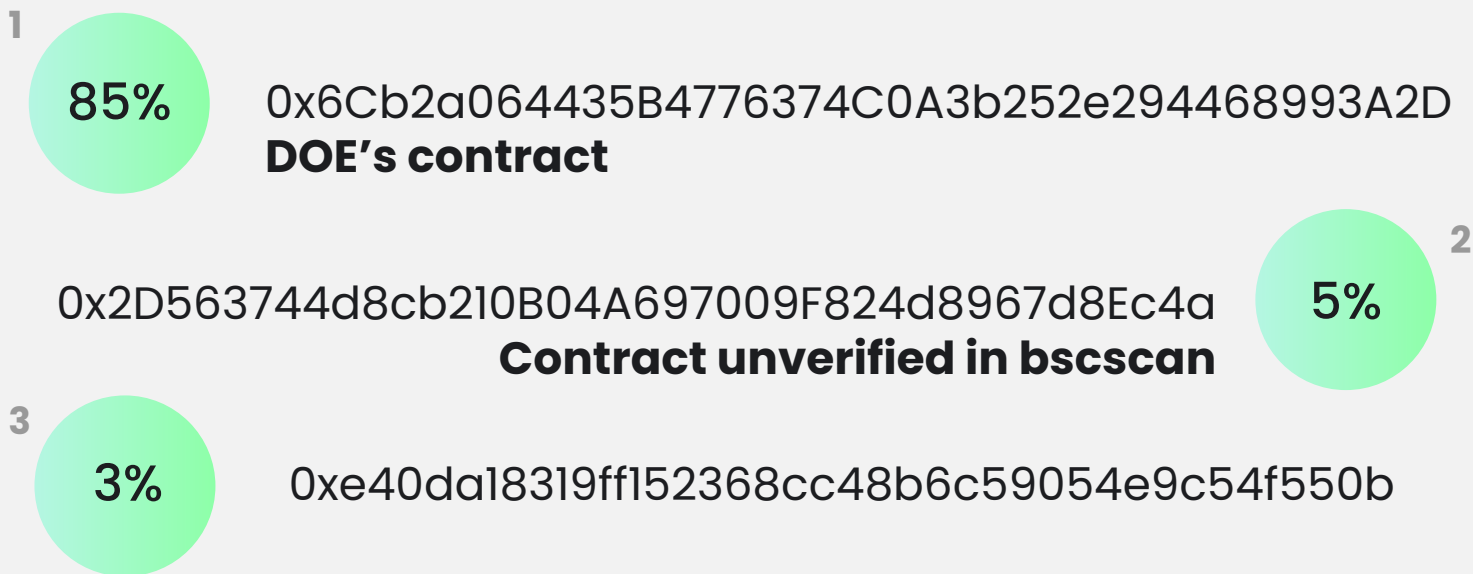
Calls Count	3931
External calls	1045
Internal calls	2886
Transactions count	1771
Uniq Callers	593
Days contract called	8
Last transaction time	2022-06-14 16:00:22 UTC
Created	2022-06-07 03:45:59 UTC
Create TX	0xa6d409ff6138f43c2ccc78186f398e094784 46a38de82e9784dd25c781bc5767
Creator	0xcc23d5782d36565ba08f3322e08a825be8 cfbd0e



FEATURED WALLETS

Owner address	0xa5C6c808C71Bd39CbDbdB1D86AF876F9a82a83c1
LP address	0x0B35a604004867E774D0C919FfFC724c05971d0f 100% Unlocked

TOP 3 UNLOCKED WALLETS





VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

⚠ High Risk

Owner can assign mint source address.

Owner and mint source assigned address can withdraw tokens from the contract to any address.

*85% of total supply is located into the token's contract

```
function setMintSource(address _source) public onlySafe {
    _mintSource = _source;
}

function userMint(address _uid, uint256 _amount) public returns (bool) {
    require(msg.sender == _mintSource || msg.sender == owner);

    // 20%这样分: 5%技术, 5%股东分红, 10%LP分红
    uint256 _engineerFee = _amount.mul(5).div(100);
    uint256 _sharesFee = _amount.mul(5).div(100);
    uint256 _lpFee = _amount.mul(10).div(100);

    _transfer(address(this), _engineer, _engineerFee);
    _transfer(address(this), _shares, _sharesFee);
    _transfer(address(this), _lpDividend, _lpFee);

    _amount = _amount.sub(_engineerFee).sub(_sharesFee).sub(_lpFee);

    _transfer(address(this), _uid, _amount.div(2));
    _assignMintBonus(_uid, _amount.sub(_amount.div(2)));
}
```



FOUND THREATS

⚠ High Risk

Owner can disable trading, making it impossible to sell.

```
function setEnableSwapTime(uint256 _time) public onlySafe {
    _swapEnableTime = _time;
}

function _transfer(address sender, address receipt, uint256 amount)
    internal returns (bool) {
    require(sender != address(0), "BEP20: transfer from the zero address");
    require(receipt != address(0), "BEP20: transfer to the zero address");

    if (_isSwap(sender)) {
        if (block.timestamp < _swapEnableTime) {
            if (_isExcluded[receipt]) {
                uint256 _totalValue = amount.mul(tokenPrice()).div(1e18);
                if (_excludedLimit[receipt].add(_totalValue) > 100e18) {
                    revert("Overflow");
                }
                _excludedLimit[receipt] += _totalValue;
                _transferBuy(sender, receipt, amount);
            } else {
                revert("transaction not opened");
            }
        }
    }
    .....
}
```

Owner can blacklist address, making it impossible to sell.

```
function setRobot(address _uid, bool _status) public onlySafe {
    require(_robots[_uid] != _status);
    _robots[_uid] = _status;
}
```



FOUND THREATS

⚠ Medium Risk

Owner can change token holdings criteria for bonuses.

```
function setHolderToken(uint256 _num1, uint256 _num2) public onlySafe {
    _holderToken1 = _num1;
    _holderToken2 = _num2;
}

function _assignBonus(address _sender, address _uid, uint256 _amount) internal {
    uint256 _level = 1;
    uint256 _total;
    while (users[_uid].pid != address(0)) {
        if (_balances[users[_uid].pid] >= _holderToken1) {
            _balances[users[_uid].pid] = _balances[users[_uid].pid].add(
                _amount.mul(2).div(1000)
            );
            emit Transfer(_sender, users[_uid].pid, _amount.mul(2).div(1000));
            _total = _total.add(_amount.mul(2).div(1000));
        }
        if (_level == 10) break;
        _uid = users[_uid].pid;
        _level++;
    }
    .....
}
```



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

Double Eagle

GOOD PRACTICES FOUND

- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner can set a transaction limit
- ✓ The smart contract utilizes "SafeMath" to prevent overflows
- ✓

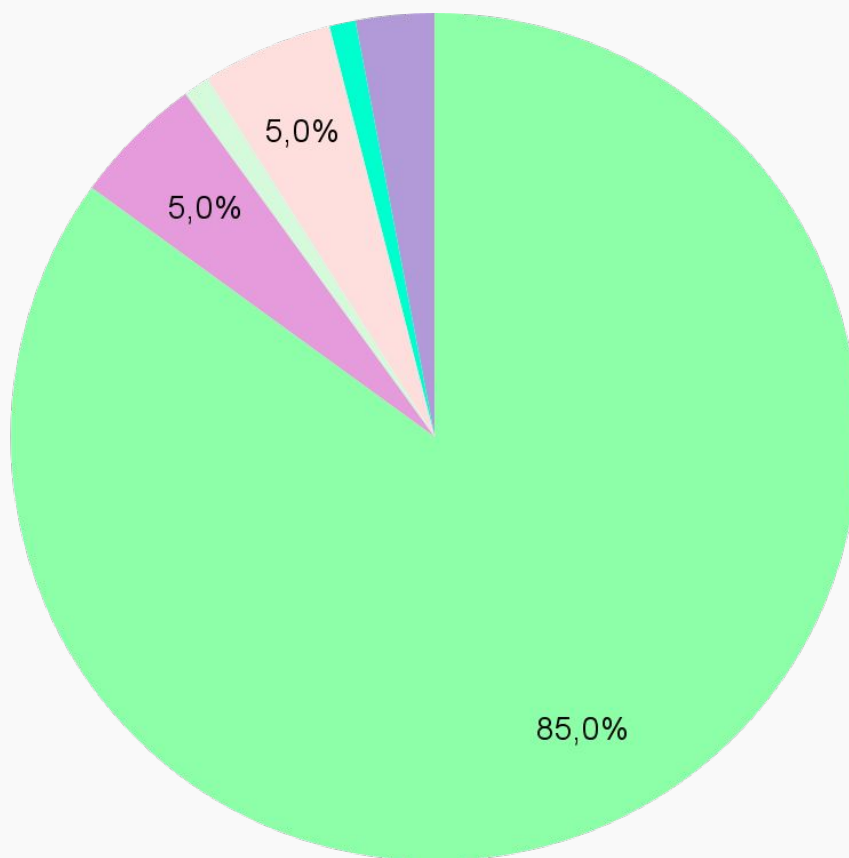


*The following tokenomics are based on the project's whitepaper and/or website:

- 85% - Mining
- 5% - IDO
- 3% - Institutions investment
- 1% - Shareholders
- 5% - Flow pool
- 1% - Market value management

Token Distribution

- Mining
- IDO
- Shareholders
- Flow pool
- Market value
- Institutions investment



TOKENOMICS



THE TEAM

! The team is
anonymous

KYC INFORMATION

! No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



**Website URL**

<https://doubleeagle.io/>

Domain Registry

<https://www.godaddy.com>

Domain Expiration

Expires on 2023-04-30

Technical SEO Test

Passed

Security Test

Passed. SSL certificate present

Design

Appropriate color scheme
and and graphics.

Content

Confusing, can be hard to
understand by new users.

Whitepaper

Confusing, semantic and
grammar mistakes. ⚠️

Roadmap

No ⚠️

Mobile-friendly?

Yes



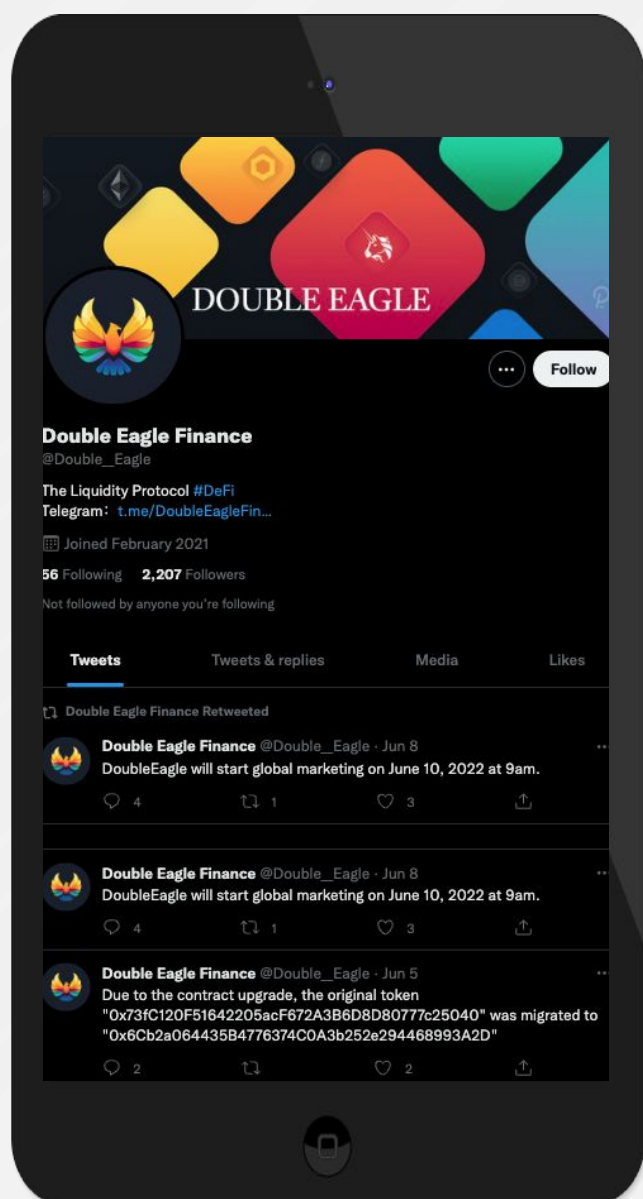
doubleeagle.io



SOCIAL MEDIA & ONLINE PRESENCE

ANALYSIS

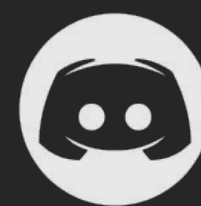
The social media presence seems lacking activity from the project owners. Follower count is OK.



Twitter

https://twitter.com/Double_Eagle

- 2 207 followers
- Not very active, few posts every few months ⚠️



Discord

- Not available



Telegram

<https://t.me/DoubleEagleFinance>

- 2 442 members, botted ⚠️
- Chat consists mainly of spam messages ⚠️



Medium

<https://medium.com/double-eagle-finance>

- Active
- Monthly reports along with other articles



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



SPYWOLF.CO



SPYWOLF.NETWORK



@SPYWOLFNETWORK



@SPYWOLFOFFICIAL



@SPYWOLFNETWORK



@SPYWOLFNETWORK



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.